CLAIMS

We claim:

1. A method of decrypting data stored on a storage medium using an encryption/decryption core embedded on a data storage engine, the method comprising:

generating an internal key using the data storage engine;

retrieving a medium key stored on the storage medium using the internal key;

generating a combination key by combining the medium key with the internal key;

decrypting a first portion of data stored on the storage medium using said first combination key.

2. The method of Claim 1 wherein the retrieving a medium key stored on the storage medium further comprises:

decrypting a master media key

generating the medium key from the master media key;

3. The method of Claim 1 wherein the internal key is generated by a pseudo-random number generator.

4. The method of Claim 2 wherein the master media key is decrypted using triple DES for two keys, wherein a first key is a first internal key and a second key is a second internal key.

5. The method of Claim 2 wherein the master media key is a 256-bit random number and the plurality of medium keys are generated by dividing the master media key into a plurality of 64-bit numbers.

6. The method of Claim 1 wherein the combination key is generated by combining the internal key with the medium key in an exclusive OR function.

7. The method of Claim 1 wherein the first portion is decrypted using triple DES for two keys, wherein a first key is the combination key and a second key is an internal key.

8. The method of Claim 2 wherein the plurality of medium keys comprises a mastered system area key, a writable system area key, and a file system information key.

9. The method of Claim 2 further comprising:

generating an additional internal key.

10. The method of Claim 9 wherein:

the plurality of medium keys comprises a mastered system area key;

the first portion of data comprises mastered data;

generating a combination key further comprises combining the mastered system area key with the internal key in an XOR function; and

decrypting the first portion further comprises using triple DES with two keys, wherein the first key is the combination key and the second key is the additional internal key.

11. The method of Claim 9 wherein:

the plurality of medium keys comprises a writable system area key;

the first portion of data comprises unmastered data;

generating a first combination key further comprises combining the writable system area key with the internal key in an XOR function; and

decrypting the first portion further comprises using triple DES with two keys, wherein the first key is the combination key and the second key is the additional internal key.

12. The method of Claim 11 further comprising:

storing a second portion of data on said unmastered area; and

encrypting the second portion of data using single DES, wherein the key is the combination key.

13. The method of Claim 9 wherein the plurality of medium keys comprises a file system information key, the method further comprising:

generating an additional combination key by combining the file system information key with the internal key in an XOR function;

decrypting a file system stored on the storage medium;

decrypting a file pointer linking the file system to the first portion of data using triple DES with two keys, wherein the first key is the second combination key and the second key is the additional internal key.

14. A method of decrypting data using a data storage engine comprising a data buffer and an ASIC, the ASIC having an encryption/decryption engine and a pseudo-random number generator, and the data being stored on a storage medium, the method comprising:

generating a plurality of internal keys using the pseudo-random number generator;

decrypting a master media key and a file system structure corresponding to a first portion of the data using at least one internal key;

generating a plurality of medium keys from the master media key;

generating a plurality of combination keys from the plurality of medium keys and the plurality of internal keys;

decrypting a first portion of the data using a first combination key.

15. The method of Claim 14 wherein the pseudo-random number generator comprises a logical feedback shift register, and wherein "generating a plurality of internal keys" further comprises:

seeding the logical feedback shift register with a seed stored in a flash memory.

16. The method of Claim 14 further comprising:

decrypting a plurality of file pointers linking the file system structure to the data using a second combination key, wherein the plurality of decrypted file pointers is stored within the ASIC.

17. The method of Claim 14 wherein said first portion comprises mastered data, the method further comprising:

encrypting a second portion of data, the second portion comprising unmastered data.

18. The method of Claim 17 wherein:

said decrypting a first portion of data further comprises decrypting using triple DES with two keys, wherein a first key is the first combination key and the second key is a first internal key; and

said encrypting further comprises encrypting using single DES, wherein the key is a second combination key.

19. The method of Claim 14 further comprising

decrypting a second portion of the data using a second combination key, wherein the first portion comprises mastered data and the second portion comprises data saved by a user.

20. A method of encrypting data stored on a storage medium using an encryption/decryption core embedded on a data storage engine, the method comprising:

generating a plurality of internal keys using the data storage engine;

decrypting a master media key stored on the storage medium using at least one of the plurality of internal keys;

generating a plurality of medium keys from the master media key;

generating a first combination key by combining a medium key with an internal key;

encrypting a portion of unmastered data using said first combination key;

storing the portion on the storage medium.

21. The method of Claim 20 wherein encrypting a first portion further comprises encrypting using single DES.

22. A method of decrypting data stored on a storage medium using a data storage engine, the method comprising:

decrypting a file system structure corresponding to the data, the file system structure comprising at least one file;

decrypting a file pointer, the file pointer indicating a location on the storage medium of a file in the file system structure;

retrieving a portion of the data from the location indicated by the file pointer.

23. The method of Claim 22 further comprising decrypting the portion of data stored at the location indicated by the file pointer.

24. The method of Claim 22 wherein the data storage engine comprises an application specific integrated circuit and a data buffer, wherein the file pointer is double encrypted, and wherein "decrypting a file pointer" further comprises:

decrypting the double encrypted file pointer, such that the file pointer is single encrypted;

storing the single encrypted file pointer in the data buffer;

retrieving the single encrypted file pointer from the data buffer;

decrypting the single encrypted file pointer within the application specific integrated circuit.

a4

25. The method of Claim 24 further comprising:

sending the portion of data retrieved from the location indicated by the file pointer to the data buffer.